UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 09/10/2009
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
KANE, CORDELIA P	
ART UNIT	PAPER NUMBER
2432	
NOTIFICATION DATE	DELIVERY MODE
09/10/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	**Application No.** 10/752,420	**Applicant(s)** ROSE ET AL.	
	Examiner CORDELIA KANE	**Art Unit** 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-24,26-28 and 50-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-24,26-28 and 50-52* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on Jul 31, 2009 has been entered.

Response to Arguments

2. Applicant's arguments filed July 31, 2009 have been fully considered but they are not persuasive. Applicant argues that claims 14 – 21 are statutory. However, even though claims 14 - 21 recite a device, no hardware is specifically recited in the claims. As taught in applicants specification paragraph [0064], the invention can be performed using software only. Therefore the claims are non-statutory. In addition, it is noted that the reference to Bilski is misplaced because the claims are not method claims.

3. Applicant goes on to argue that Lewis fails to teach or suggest disabling the private key when the replacement second private key is recreated and used for authentication. However, Lewis teaches that the private key is used to sign the key replacement message (column 3, lines 61-62) and the replacement message signals a key replacement, when the active key is discarded (column 3, lines 25-26). Therefore the replacement private key is used for authentication before being discarded.

4. Applicant goes on to argue that Brennan teaches a master key instead of a private key, and therefore cannot teach preventing retransmission of the private key. However, Brennan teaches keeping a cryptographic key secure, including a private key (column 2, lines 32-35). Therefore Brennan teaches preventing retransmission of the private key.

5. Applicant's arguments with respect to the other rejections have been considered but are moot in view of the new ground(s) of rejection.

Election/Restrictions

6. Newly submitted claim 52 is directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: It is drawn to the previously withdrawn species 2: using a previous key and a system parameter to create the second key.

7. Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claim 52 is withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 101

9. Claims 14 - 21,and 40 - 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In the specification applicant defines the means to include software only [0064].

Claim Rejections - 35 USC § 103

10. Claims 1 – 3, 5 – 24, 26 – 28, 50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis's US Patent 5,761,306, and further in view of Sudia US Patent 6,009,177. Referring to claims 1, 14 and 22, Lewis teaches:

a. Creating a first private key and corresponding public key (column 6, lines 14-16).

b. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 6, lines 14-17).

c. Disabling the first private key when the second private key is used (column 3, lines 25-26, and 61-62).

d. Transmitting the second public key concurrent with the first public key (column 3, lines 23-25, column 4, lines 12-14).

e. Using the first private key for authentication (column 8, lines 40-49).

11. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks

communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

12. Referring to claims 2 and 23, Sudia teaches:

f. Creating at least two shares of the second private key at the device (column 18, lines 12-14).

g. Outputting each share to a different entity (column 18, lines 37-39).

13. Referring to claims 3, 16, and 24, Lewis teaches using the second private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Sudia teaches re-creating the private key using the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

14. Referring to claims 5 and 17, Lewis teaches:

h. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 7, lines 31-37).

i. Outputting the third public key (column 7, lines 59-65).

15. Referring to claim 6, Lewis teaches using the third private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

16. Referring to claim 7, Lewis teaches that the second private and public keys are created independently from the first private and public keys (column 7, lines 59-60).

17. Referring to claims 8 and 18, Lewis teaches:

j. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 7, lines 31-37).

k. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 7, lines 31-37).

l. Outputting the third and fourth public keys (column 7, lines 59-65).

18. Lewis fails to teach outputting the fourth private key once such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The

suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

19. Referring to claim 9, Lewis teaches:

m. Disabling use of the second private key for authentication (column 3, lines 25-26).

n. Using the third private key for authentication (column 8, lines 40-49).

o. Using the fourth private key for authentication (column 8, lines 40-49).

20. Lewis fails to teach recreating the fourth private key. Sudia teaches re-creating the private key using the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

21. Referring to claim 10, Sudia teaches preventing retransmission of the second private key (column 42, lines 14-19).

22. Referring to claims 11, 19, and 26, Lewis discloses:

p. Receiving a first public key (column 10, lines 1-4).

q. Receiving a second public key concurrent with receipt of the first public key, the second public key associated with the first public key (column 10, lines

1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated and used for authentication (column 3, lines 25-26, column 4, lines 12-14).

r. Using the first public key for authentication (column 8, lines 40-49).

s. Using the second public key for authentication if the first public key fails (column 8, lines 58-64).

23. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

24. Referring to claims 12, 20 and 27, Lewis teaches receiving a third public key from the device, the third public key associated with the second public key (column 7, lines

31-37), if the first public key fails and the second key results in successful authentication (column 8, lines 58-64).

25. Referring to claims 13, 21, and 28, Lewis teaches a third public key and a fourth public key from the device (column 7, lines 31-37), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 8, lines 58-64).

26. Referring to claim 15, Sudia teaches:

t. Creating at least two shares of the private key (column 18, lines 12-14).

u. Wirelessly (column 26, line 65) outputting each share once to a different entity(column 18, lines 37-39), wherein subsequent outputting of the second private key is prevented (column 42, lines 14-19).

27. Referring to claim 50, Lewis teaches:

v. A processor configured to generate a first private key and corresponding first public key, the processor configured to generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 6, lines 14-17).

w. A storage medium coupled to the processor to store the first private key (column 6, lines 14-17).

x. A transmitter to output the second public key to the device concurrent with outputting the first public key (column 10, lines 1-4) and disable the first private key when the second private key is created and used for authentication (column 3, lines 25-26, column 4, liens 12-14).

y. Wherein the processor uses the first private key for authentication of the device (column 8, lines 40-49).

28. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

29. Referring to claim 51, Lewis teaches:

z. A receiver configured to receive a first public key from a device and receiving a second public key from the device concurrent with receipt of the first public key, the second public key associated with the first public key (column 10, lines 1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated and used for authentication (column 3, lines 25-26, column 4, lines 12-14).

aa. A storage medium coupled to the receiver configured to store the first and second public keys (column 10, lines 1-4).

bb. A processor coupled to the receiver, the processor configured to use the first public key for authentication (column 8, lines 40-49), the processor configured to use the second public key for authentication if the first public key fails (column 8, lines 58-64).

30. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Lewis and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Sudia before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is

(571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432